IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

IN RE EQUIFAX, INC., CUSTOMER DATA SECURITY BREACH LITIGATION	MDL DOCKET NO. 2800 1:17-md-2800-TWT ALL CASES

OPINION AND ORDER AND SUGGESTION OF REMAND

This is a data breach case. It is before the Court on the Defendants' Motion to Dismiss [Doc. 1220]. For the reasons set forth below, the Defendants' Motion to Dismiss [Doc. 1220] is GRANTED with respect to Douglas Adams [No. 1:19-cv-3682-TWT], Alice Flowers [No. 1:10-cv-5703-TWT], Edward Hutchinson [No. 1:19-cv-5706-TWT], Ruby Hutchinson [No. 1:19-cv-5705-TWT], Raymond Silva [No. 1:19-cv-3825-TWT], Christopher Eustice and Cathy Eustice [No. 1:19-cv-3128-TWT], Christopher Eustice and David Eustice [No. 1:19-cv-3129-TWT], and Christopher Eustice and Travis Hubbard [No. 1:19-cv-3130-TWT]. The Court GRANTS in part and DENIES in part the Defendants' Motion to Dismiss [Doc. 1220] with respect to Audella Patterson [No. 1:19-cv-5529], Brett Joshpe [No. 1:19-cv-3595-TWT], Richard Khalaf [No. 1:19-cv-3830], and Anna Lee [No. 1:18-cv-4698-TWT]. The Court suggests to the Judicial Panel on Multidistrict Litigation that the actions of Audella Patterson [No. 1:19-cv-5529], Brett Joshpe [No. 1:19-cv-3595-TWT], Richard Khalaf [No. 1:19-cv-3830], and Anna Lee [No. 1:18-cv-4698-TWT] be remanded to the transferor courts for further proceedings.

I. Background

On September 7, 2017, Defendant Equifax Inc. announced that hackers had stolen the personal and financial information of nearly 150 million Americans from its computer networks in one of the largest data breaches in history (the "Data Breach"). *See In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1308 (N.D. Ga. 2019). The Data Breach spawned more than 300 class actions against Equifax Inc., Equifax Information Services, LLC, and Equifax Consumer Services LLC (collectively, "Equifax"), which were consolidated and transferred to this Court as part of a multidistrict litigation ("MDL"). The Court established separate tracks for the consumer and financial institution claims and appointed separate legal teams to lead each track. In the consumer track, the Consumer Plaintiffs and Equifax reached a class action settlement of all claims arising out of the Data Breach, which the Court approved, and the Eleventh Circuit affirmed (except on the narrow issue of incentive awards), in an order dated March 17, 2020. *See In re Equifax Customer Data Sec. Breach Litig.*, 2020 WL 256132 (N.D. Ga. Mar. 17, 2020), *aff'd in part, rev'd in part*, 999 F.3d 1247 (11th Cir. 2021).[1]

A small number of Consumer Plaintiffs (the "Opt-Out Plaintiffs") who filed complaints in the MDL requested to be excluded from the class action settlement. Equifax now moves to dismiss their complaints, described below, for failure to state

[1] On November 1, 2021, and January 10, 2022, the Supreme Court denied two petitions for writ of certiorari to review the Eleventh Circuit's decision.

a claim under Federal Rule of Civil Procedure 12(b)(6).

Opt-Out Plaintiffs Douglas Adams, Alice Flowers, Edward Hutchinson, Ruby Hutchinson, Audella Patterson, and Raymond Silva assert contract claims based on Equifax's alleged "commercial acquiescence" to a "Notice of Default." (Equifax's Br. in Supp. of Equifax's Mot. to Dismiss, Ex. 1, Pt. 1 at 5; *id.*, Ex. 1, Pt. 2 at 107, 143, 188; *id.*, Ex. 1, Pt. 3 at 57, 91.)[2] Following the Data Breach, each individual mailed Equifax a "Conditional Acceptance" letter that requested "Proof of Claim" about its knowledge of, response to, and liability for the incident. The letter provided that "[y]our non-response will equate to commercial acquiescence to the terms outlined . . . in a final Affidavit and Notice of Default." (*E.g.*, *id.*, Ex. 1, Pt. 1 at 8-9.) After not responding to the Conditional Acceptance and a second letter, Equifax was sent an "Affidavit and Notice of Default" stating that Equifax "has willingly, knowingly, intentionally, or voluntarily agreed and acquiesced through its non-response to the facts stated herein." Those facts include that Equifax is "liable to me . . . for damages no less than a minimum of $75,000,000.00[.]" (*E.g.*, *id.*, Ex. 1, Pt. 1 at 14.) The Opt-Out Plaintiffs allege that Equifax is now "in default under contract." (*E.g.*, *id.*, Ex. 1, Pt. 1 at 5.)

In addition to her commercial acquiescence claim, Patterson raises a claim for negligence based on Equifax's "careless disregard for safeguarding the sensitive data

[2] Unless stated otherwise, all citations to the exhibits to Equifax's Motion to Dismiss refer to the PDF page number.

it collected to unjustly financially benefit from the data it collected, stored, and sold." (*Id.*, Ex. 1, Pt. 3 at 55.) That "careless disregard," she alleges, "put [her] at risk of identity theft for the rest of her life." (*Id.*, Ex. 1, Pt. 3 at 55.) Patterson also asserts a claim for unjust enrichment on the grounds that Equifax "prioritized growth and profits over protecting the [personal identifying information ("PII")] of consumers," and that Equifax stands to gain new credit monitoring customers (and thus more revenue) as a result of the Data Breach. (*Id.*, Ex. 1, Pt. 3 at 56-57.) Finally, Patterson accuses Equifax of violating the California Customer Records Act ("CCRA") because it failed to publicly disclose the Data Breach in a "timely and accurate" manner. (*Id.*, Ex. 1, Pt. 3 at 55-56.) She alleges that, as a direct and proximate cause of the delayed notice, she "suffered identity theft and aggravated identity theft damages," for which she now seeks actual damages and injunctive relief under the statute. (*Id.*, Ex. 1, Pt. 3 at 56.)

Three of the opt-out complaints were filed by Christopher Eustice, on behalf of himself and Cathy Eustice, David Eustice, and Travis Hubbard (the "Eustice Plaintiffs"), in Texas state court. (*Id.*, Ex. 1, Pt. 1 at 37, 100; *id.*, Ex. 1, Pt. 2 at 56.) The Eustice Plaintiffs raise the following identical, verbatim claims against Equifax:

- Willful Injury – [Fair Credit Reporting Act ("FCRA")] Section 623 and Cushman V. Transunion Corporation US Court of Appeals for the Third Circuit Court Case 115 F.3d 220 June 9, 1997, Filed (D.C. No. 95-cv-01743);
- Violation(s) of FCRA, including but not limited to Part (A)(5)(B)(ii) and FCRA Section 611 Part (A)(1);
- Breach of Oral Contract for a Service not lasting more than a year and Breach of Written Contract;

- Violations(s) [sic] of Texas Business and Commerce Code ("TBCC") ch. 20; and
- Personal Injury Tort Claims.

(*E.g.*, *id.* Ex. 1, Pt. 1 at 37.) The complaints contain no factual assertions in support of these claims; instead, Christopher Eustice attaches a list of press statements, articles, and other documents with "relevant information . . . to [the] breach of [his] client's private information[.]"[3] (*E.g.*, *id.* Ex. 1, Pt. 1 at 41-42.) In an accompanying affidavit, Christopher Eustice states that the Equifax "vulnerability was known for at least four months to the cyber security industry before Equifax was hacked and took remedial measures to protect consumer information." (*E.g.*, *id.* Ex. 1, Pt. 1 at 41.) The Eustice Plaintiffs seek $9,975 each in monetary damages. (*Id.*, Ex. 1, Pt. 1 at 37, 100; *id.*, Ex. 1, Pt. 2 at 56.)

Brett Joshpe and Richard Khalaf bring claims for negligence and violations of New York General Business Law ("NYGBL") Section 349 and the FCRA. (*Id.*, Ex. 1, Pt. 3 at 1-2, 15-16.) They have allegedly "suffered financial, emotional and reputational damages" as "a direct and proximate result of the data breach[.]" (*Id.*, Ex. 1, Pt. 3 at 13, 26.) Among their stated damages, Joshpe and Khalaf have received harassing and fraudulent phone calls; their credit ratings have been damaged such that Joshpe was denied a credit card in December 2018; Joshpe's PayPal account has been used in unauthorized transactions; fraudulent bank and credit card accounts

[3] Although Christopher Eustice refers to the other Eustice Plaintiffs as his "clients" and to himself as their "authorized agent," Equifax states that he is in fact not a licensed attorney. (Equifax's Br. in Supp. of Equifax's Mot. to Dismiss, at 5.)

have been opened in Joshpe's name; Khalaf has been targeted with check, credit card, and tax return fraud; and Joshpe's personal Gmail account has been hacked and used to send embarrassing messages to business and personal contacts. (*Id.*, Ex. 1, Pt. 3 at 8, 22.) Joshpe and Khalaf also claim to have expended "significant emotional and financial resources" in an unsuccessful effort to mitigate the effects of the Data Breach. (*Id.*, Ex. 1, Pt. 3 at 8-9, 22-23.) They seek no less than $1,000,000 in monetary damages on each count as well as litigation expenses, punitive damages, and injunctive relief. (*Id.*, Ex. 1, Pt. 3 at 14, 26.)

Finally, Anna Lee filed an action in New York state court asserting claims for negligence and violations of NYGBL Section 349 and the FCRA. (*Id.*, Ex. 1, Pt. 3 at 36-40.) Her injuries include "the loss of [her] legally protected interest in the confidentiality and privacy of [her] Personal Information" as well as "a significant risk of harm or threat of harm in the future," citing unspecified reports that information from the Data Breach is for sale on the Dark Web. (*Id.*, Ex. 1, Pt. 3 at 38-39.) Lee has also allegedly "spent numerous hours monitoring [her] accounts and addressing issues arising from the . . . Data Breach." (*Id.*, Ex. 1, Pt. 3 at 37.) Her complaint requests damages in the amount of $25,000. (*Id.*, Ex. 1, Pt. 3 at 40.)

II. Legal Standard

A complaint should be dismissed under Rule 12(b)(6) only where it appears that the facts alleged fail to state a "plausible" claim for relief. *Ashcroft v. Iqbal*, 129 S. Ct. 1937, 1949 (2009); Fed. R. Civ. P. 12(b)(6). A complaint may survive a motion

to dismiss for failure to state a claim, however, even if it is "improbable" that a plaintiff would be able to prove those facts; even if the possibility of recovery is extremely "remote and unlikely." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 556 (2007). In ruling on a motion to dismiss, the court must accept the facts pleaded in the complaint as true and construe them in the light most favorable to the plaintiff. *See Quality Foods de Centro Am., S.A. v. Latin Am. Agribusiness Dev. Corp., S.A.*, 711 F.2d 989, 994-95 (11th Cir. 1983); *Sanjuan v. American Bd. of Psychiatry & Neurology, Inc.*, 40 F.3d 247, 251 (7th Cir. 1994) (noting that at the pleading stage, the plaintiff "receives the benefit of imagination"). Generally, notice pleading is all that is required for a valid complaint. *See Lombard's, Inc. v. Prince Mfg., Inc.*, 753 F.2d 974, 975 (11th Cir. 1985). Under notice pleading, the plaintiff need only give the defendant fair notice of the plaintiff's claim and the grounds upon which it rests. *See Erickson v. Pardus*, 551 U.S. 89, 93 (2007) (citing *Twombly*, 550 U.S. at 555).

III. Discussion

A. Choice of Law

At the outset, the Parties dispute which state's law should govern the Opt-Out Plaintiffs' common law claims. On the one hand, Joshpe and Khalaf contend that, under 28 U.S.C. § 1407, the transferee court in an MDL must apply the state law that the transferor court would have applied, including its choice-of-law rules. (*E.g.*, Joshpe's Br. in Opp'n to Equifax's Mot. to Dismiss, at 9-10.) They then summarily conclude that New York law governs their negligence claims, without showing any of

the choice-of-law analysis required to reach that result. (*E.g.*, *id.* at 11.) On the other hand, Equifax takes the position that New York's choice-of-law rules warrant the application of Georgia substantive law here. (Reply Br. in Supp. of Equifax's Mot. to Dismiss, at 7-11.) In tort cases, New York has adopted an "interest analysis" that is designed "to give controlling effect to the law of the jurisdiction which, because of its relationship or contact with the occurrence or the parties, has the greatest concern with the specific issue raised in the litigation." *Finance One Pub. Co. Ltd. v. Lehman Bros. Special Fin., Inc.*, 414 F.3d 325, 337 (2d Cir. 2005) (citation omitted). Relevant factors include "[t]he contacts of the parties and occurrences with each jurisdiction . . . the policies underlying each jurisdiction's rules, the strength of the governmental interests embodied in these policies, and the extent to which these interests are implicated by the contacts." *Id.*

There are two overarching principles under the interest-analysis test which are particularly relevant to this case. First, when dealing with a conduct-regulating law, such as negligence, there is a presumption that "the law of the jurisdiction where the allegedly tortious acts occurred will generally apply because that jurisdiction has the greatest interest in regulating behavior within its borders." *Licci ex rel. Licci v. Lebanese Canadian Bank, SAL*, 739 F.3d 45, 49 (2d Cir. 2013) (citation and alteration omitted); *see also Bak v. Metro-North R.R. Co.*, 100 F. Supp. 3d 331, 338 (S.D.N.Y. 2015) ("The law of negligence is a conduct-regulating rule because it seeks to hold defendants to a standard of care."). Second, and relatedly, when those tortious acts

arise out of corporate policies or decision-making, the conduct is deemed to have taken place at the corporation's principal place of business or nerve center, unless demonstrated otherwise. *See, e.g.*, *In re Air Crash Near Clarence Ctr., N.Y., on Feb. 12, 2009*, 798 F. Supp. 2d 481, 490-91 (W.D.N.Y. 2001) (noting most of the corporate acts underlying the plaintiff's claims, such as an airline's failure to implement adequate safety programs and negligent hiring and training of flight crews, occurred at its Virginia headquarters); *Deutsch v. Novartis Pharms. Corp.*, 723 F. Supp. 2d 521, 525 (E.D.N.Y. 2010) (reasoning a pharmaceutical company made decisions at its New Jersey headquarters to conduct inadequate clinical trials, conceal information from regulators, and increase a drug's dosage and dosing schedule to excessive levels).

Here, Joshpe and Khalaf allege that Equifax "willfully and/or negligently failed to address the known vulnerability in their software that made the attack possible in the first place, failed to detect the attack for 76 days, and then failed to inform . . . members of the public for over one month after the data breach was discovered." (Equifax's Br. in Supp. of Equifax's Mot. to Dismiss, Ex. 1, Pt. 3 at 7, 21.) It is undisputed that these corporate decisions were made at Equifax's principal place of business in Atlanta, Georgia. (*Id.*, Ex. 1, Pt. 3 at 2, 16.) Therefore, the Court presumes that Georgia substantive law applies based on that state's superior interest in regulating behavior within its borders. Even if Joshpe and Khalaf may have suffered some injuries at their domiciles in New York, the place of the wrongful conduct usually takes precedence over the place of the injury. *Licci*, 739 F.3d at 50-51. Indeed,

because Equifax maintains personal information on hundreds of millions of consumers nationwide, this case offers "a quintessential example of when the location of the plaintiff's injury is fortuitous and the law of the place where the defendant's conduct occurred should be given more weight." *Mackey v. Belden, Inc.*, 2021 WL 3363174, at *3 (E.D. Mo. Aug. 3, 2021); *see also Gordon v. Chipotle Mexican Grill, Inc.*, 344 F. Supp. 3d 1231, 1244 (D. Colo. 2018); *Veridian Credit Union v. Eddie Bauer, LLC*, 295 F. Supp. 3d 1140, 1155 (W.D. Wash. 2017).

For these reasons, the Court concludes that Joshpe's and Khalaf's negligence claims are governed by Georgia, not New York, law. Aside from Joshpe and Khalaf, Adams is the only other Opt-Out Plaintiff who filed a response (though untimely) to Equifax's Motion to Dismiss. Because he does not object to Equifax's choice-of-law analysis, the Court will also apply Georgia law to his and the non-responsive Opt-Out Plaintiffs' common law claims. (Equifax's Br. in Supp. of Equifax's Mot. to Dismiss, at 8-9.) *See also In re Equifax*, 362 F. Supp. 3d at 1311-12 (applying Georgia law to the Consumer Plaintiffs' common law claims);

B. Rule 8's Pleading Standard

Next, Equifax contends that the complaints of Adams, Flowers, E. Hutchinson, R. Hutchinson, Patterson, Silva, and the Eustice Plaintiffs should be dismissed under Rule 8. (Equifax's Br. in Supp. of Equifax's Mot. to Dismiss, at 10 (quoting *Ashcroft*, 556 U.S. at 678).) Under Rule 8(a)(2), a plaintiff must provide "a short and plain statement of the claim" showing that he is entitled to relief. Fed. R. Civ. P. 8(a)(2).

The purpose of this requirement is to "give the defendant fair notice of what the claim is and the grounds upon which it rests." *Twombly*, 550 U.S. at 555 (citation and alteration omitted). Although a complaint need not include detailed factual allegations, the "grounds" must be "more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Id.* In cases involving pro se plaintiffs such as this one, courts must hold their complaints, however inartfully pleaded, "to less stringent standards than formal pleadings drafted by lawyers." *Arrington v. Wells Fargo*, 842 F. App'x 307, 311 (11th Cir. 2020) (quotation marks, citation, and alteration omitted).

First, Equifax argues that Adams, Flowers, E. Hutchinson, R. Hutchinson, and Silva improperly use "boilerplate language" and "pseudo-legal documents" to plead their commercial acquiescence claims. (Defs.' Br. in Supp. of Defs.' Mot. to Dismiss, at 10.) In the Court's view, this argument bears less on the issue of adequate notice under Rule 8(a)(2) and more on the issue of legal sufficiency under Rule 12(b)(6). The challenged complaints state in unison that

> Defendents [sic] were afforded commercial grace and an opportunity to provide the requested proofs of claims and failed to provide proofs[ ]of claim as enumerated in the Conditional Acceptance sent to Defendant via certified mail . . . . Defendents [sic] were then sent a Notice of Fault and Opportunity to Cure the fault and failed to respond. Through Defendents [sic] non-response and sielnece [sic], the Defendants have quietly agreed to all of the facts as outlined in the Notice of Default.

(*E.g.*, *id.*, Ex. 1, Pt. 1 at 5.) Attached to each complaint are the referenced documents with proof of receipt by Equifax, which recount in full the allegedly agreed-upon facts

and the basis for construing Equifax's silence as acceptance. (*E.g.*, *id.*, Ex. 1, Pt. 1 at 8-16.) Whether these allegations and documents make out a viable claim for relief is a separate question, but they at least provide a short, plain statement of the claim sufficient to meet Rule 8's liberal pleading requirements.

Similarly, Equifax characterizes Patterson's complaint as a mere "recitation[] of the elements of legal claims and quotations of publicly available sources, none of which set forth a coherent claim for relief." (*Id.* at 11.) The Court views the complaint in a different light. First, Patterson's commercial acquiescence claim passes muster under Rule 8 for the same reasons set forth above. Second, her negligence claim alleges that Equifax breached a duty of care under Georgia case law by failing "to exercise reasonable ordinary care of the private PII data entrusted to its care[.]" (*Id.*, Ex. 1, Pt. 3 at 54-55.) Equifax's conduct, she continues, "put [her] at risk of identity theft for the rest of her life." (*Id.*, Ex. 1, Pt. 3 at 55.) Patterson then asserts on her unjust enrichment claim that the Data Breach was the "inevitable result of EQUIFAX's systemic incompetence and a longstanding, lackluster approach to data security . . . . despite warnings by outside cybersecurity experts." (*Id.*, Ex. 1, Pt. 3 at 56.) Now, new credit monitoring customers allegedly present a "huge revenue opportunity" for Equifax in the wake of the Data Breach. (*Id.*, Ex. 1, Pt. 3 at 56.) Finally, in support of her CCRA claim, Patterson states that Equifax knew about the Data Breach for more than 40 days before informing the public, a delay which caused her to "suffer[] identity theft and aggravated identify theft damages." (*Id.*, Ex. 1, Pt.

3 at 55.) The Court finds that these allegations give adequate notice of the factual grounds for Patterson's claims.

Equifax fares better on its Rule 8 challenge to the Eustice Plaintiffs' complaints. On their petition forms, the Eustice Plaintiffs listed their causes of action as (1) "Willful Injury – FCRA Section 623 and Cushman V. Transunion Corporation US Court of Appeals for the Third Circuit Court Case 115 F.3d 220 June 9, 1997, Filed (D.C. No. 95-cv-01743)"; (2) "Violation(s) of FCRA, including but not limited to Part (A)(5)(B)(ii) and FCRA Section 611 Part (A)(1)"; (3) "Breach of Oral Contract for a Service not lasting more than a year and Breach of Written Contract"; (4) "Violations(s) [sic] of [TBCC] ch. 20"; and (5) "Personal Injury Tort Claims." (*E.g.*, *id.* Ex. 1, Pt. 1 at 37.) The complaints are devoid of any factual allegations but rather incorporate an "Affidavit of Evidence and Law" with publicly available articles and press releases (none specific to the Eustice Plaintiffs) and federal statutory citations. (*E.g.*, *id.* Ex. 1, Pt. 1 at 41-42.) Without more details, it is impossible to discern the basis for even a single one of the Eustice Plaintiffs' claims. For example, they fail to cite any oral or written contract that Equifax may have breached, any provision of the TBCC that Equifax may have violated, or any tort that Equifax may have committed as a result of the Data Breach.

According to Equifax, "[f]ederal courts routinely dismiss under Rule 8 pro se complaints which 'ramble and cite multiple statutes' without 'providing an explanation of Plaintiffs' legal theories.'" (*Id.* at 12 (alterations omitted) (quoting

Hayes v. Bank of N.Y. Mellon, 2014 WL 3887922, at *6, 8 (N.D. Ga. Aug. 6, 2014)).) Without a doubt, Rule 8 does not allow the Eustice Plaintiffs to rely on conclusory labels, absent any substantive factual allegations, to make out their claims against Equifax. Although pro se complaints are graded on a more lenient curve, it is not the Court's role "to serve as de facto counsel for a party, or to rewrite an otherwise deficient pleading in order to sustain an action." *Arrington*, 842 F. App'x at 311 (citation omitted). None of the Eustice Plaintiffs have filed a response to Equifax's Motion to Dismiss objecting to dismissal of their complaints or requesting an opportunity to replead their claims. The Court thus concludes that their complaints should be dismissed under Rule 8(a)(2). *See Weiland v. Palm Beach Cnty. Sheriff's Office*, 792 F.3d 1313, 1320 (11th Cir. 2015) (a district court has "inherent authority to control its docket and ensure the prompt resolution of lawsuits, which in some circumstances includes the power to dismiss a complaint for failure to comply with Rule 8(a)(2)").

C. Commercial Acquiescence

Shifting focus to Rule 12(b)(6), Equifax argues that all of the commercial acquiescence claims should be dismissed because Equifax did not agree to any contract. (Equifax's Br. in Supp. of Equifax's Mot. to Dismiss, at 13-14.) As described above, several of the Opt-Out Plaintiffs claim that Equifax has "quietly agreed" to the fact and amount of its liability for the Data Breach, as set forth in a series of letters. (*E.g.*, *id.*, Ex. 1, Pt. 2 at 107, 132-33; *id.*, Ex. 1, Pt. 4 at 57.) But silence, standing alone,

does not demonstrate the "mutual assent or meeting of the minds" required to create an enforceable contract. *Hart v. Hart*, 297 Ga. 709, 711-12 (2015) (citation omitted); *see also* O.C.G.A. § 13-3-1. Under Georgia's objective theory of intent, the Opt-Out Plaintiffs have not alleged facts from which a reasonable person could interpret Equifax's non-response as a manifestation of assent. *See Legg v. Stovall Tire & Marine, Inc.*, 245 Ga. App. 594, 596 (2000)[4]; *see also Davis v. Equifax, Inc.*, 2020 WL 7000971, at *2 (D.S.C. Sept. 30, 2020) (dismissing an identical claim arising out of the Data Breach for lack of assent); *Tiamson v. Equifax, Inc.*, 2020 WL 3972582, at *5 (N.D. Cal. July 14, 2020) (same). Therefore, the Court dismisses the commercial acquiescence claims of Adams, Flowers, E. Hutchinson, R. Hutchinson, Patterson, and Silva.

D. Unjust Enrichment

Equifax moves to dismiss Patterson's unjust enrichment claim for failure "to allege that she conferred a benefit on Equifax." (Equifax's Br. in Supp. of Equifax's Mot. to Dismiss, at 17 (quotation marks and citation omitted).) "[T]he theory of unjust enrichment applies when there is no legal contract and when there has been a benefit

[4] *Accord Martinez v. BaronHR, Inc.*, 265 Cal. Rptr. 3d 523, 527 (Cal. Ct. App. 2020) (outward manifestations of mutual assent are required to form a contract under California law, applicable to Patterson); *Homer v. Burman*, 743 N.E.2d 1144, 1146-47 (Ind. Ct. App. 2001) (same under Indiana law, applicable to Flowers and the Hutchinsons); *Siopes v. Kaiser Found. Health Plan, Inc.*, 312 P.3d 869, 879 (Haw. 2013) (same under Hawaii law, applicable to Silva); *Baylor Univ. v. Sonnichsen*, 221 S.W.3d 632, 635 (Tex. 2007) (same under Texas law, applicable to Adams).

conferred which would result in an unjust enrichment unless compensated." *Clark v. Aaron's, Inc.*, 914 F. Supp. 2d 1301, 1309 (N.D. Ga. 2012) (quotation marks and citation omitted).[5] To show that Equifax has financially benefited from the Data Breach, Patterson cites statements from former Equifax Chief Executive Officer Richard Smith and United States Senator Elizabeth Warren speculating that Equifax could boost revenue from its credit monitoring services due to the Data Breach. (Equifax's Br. in Supp. of Equifax's Mot. to Dismiss, Ex. 1, Pt. 3 at 56-57.) Beyond that hypothetical scenario, though, Patterson does not allege that she has paid Equifax for any product or service, or that she has conferred any other type of benefit on the company. Accordingly, her complaint fails to state a claim for unjust enrichment.

E. Negligence

Equifax seeks to dismiss the negligence claims of Joshpe, Khalaf, Lee, and Patterson on the grounds that they have not sufficiently alleged three of the four essential elements: duty of care, injury, and proximate causation. (*Id.* at 19, 25.) The Court addresses each element in turn below.

1. Duty of Care

"The threshold issue in any cause of action for negligence is whether, and to

[5] *Accord Schertzer v. Bank of Am., N.A.*, 489 F. Supp. 3d 1061, 1076 (S.D. Cal. 2020) (Under California law, "[i]n order for a plaintiff to successfully plead an unjust enrichment claim, he/she must show that a benefit was conferred on the defendant through mistake, fraud, coercion, or request.").

what extent, the defendant owes the plaintiff a duty of care." *DaimlerChrysler Motors Co., LLC v. Clemente*, 294 Ga. App. 38, 47 (2008) (citation omitted). Addressing this issue on an earlier motion to dismiss, the Court held that Equifax owed the Consumer Plaintiffs a duty "to safeguard the personal information in its custody." *In re Equifax*, 362 F. Supp. 3d at 1325. This conclusion was premised on allegations that Equifax knew about a foreseeable risk to its data security systems but failed to implement reasonable security measures. *See id.* Based on the alleged foreseeability of the Data Breach, the Court distinguished a line of cases beginning with *McConnell v. Department of Labor*, 337 Ga. App. 457 (2016) ("*McConnell I*"), which found no duty to protect personal information under Georgia statutory or case law. *See In re Equifax*, 362 F. Supp. 3d at 1322-23, 1325. Additional support for Equifax's legal duty came from federal statutes and rules governing the national credit reporting agencies and from Georgia case law recognizing a "general duty 'to all the world not to subject [others] to an unreasonable risk of harm.'" *Id.* at 1324-25, 1326 (quoting *Bradley Center, Inc. v. Wessner*, 250 Ga. 199, 201 (1982)).

According to Equifax, this analysis has been upended by the Georgia Supreme Court's latest decision in *Department of Labor v. McConnell*, 305 Ga. 812 (2019) ("*McConnell IV*"). (Equifax's Br. in Supp. of Equifax's Mot. to Dismiss, at 26.) There, the court ruled that the Georgia Department of Labor did not owe unemployment applicants—whose names, social security numbers, and other personal information were accidentally emailed to about 1,000 people—"a duty to protect their information

against negligent disclosure." *McConnell IV*, 305 Ga. at 816. The court disapproved of *Bradley Center* "to the extent that it created a general legal duty to all the world not to subject others to an unreasonable risk of harm." *Id.* (quotation marks, citation, and alteration omitted). And it held that two Georgia statutes—O.C.G.A. §§ 10-1-910 and 10-1-393.8—at most created a duty to refrain from intentional, but not negligent, disclosures of social security numbers. *Id.* (emphasis added). Following *McConnell IV*, the Eleventh Circuit has noted that the decision "seriously calls into question the existence under Georgia law of an independent common-law duty to safeguard and protect personal information." *Murray v. ILG Techs., LLC*, 798 F. App'x 486, 492 (11th Cir. 2020) (quotation marks, citation, and alteration omitted).

Despite this development in Georgia's negligence jurisprudence, the Court believes that its prior duty of care holding remains sound. As a threshold matter, *McConnell IV* did not, as Equifax contends, "definitively h[o]ld that there is no duty under Georgia law to safeguard personal information." (Equifax's Br. in Supp. of Equifax's Mot. to Dismiss, at 26.) Rather, the decision was limited to just three proposed sources of that duty: *Bradley Center* and O.C.G.A. §§ 10-1-910 and 10-1-393.8. *McConnell IV*, 305 Ga. at 815-16. Indeed, the Georgia Supreme Court recognized that "a duty might arise on these or other facts from any other statutory or common law source[.]" *Id.* at 816 n.5. That same year, the Georgia Supreme Court confirmed the narrow scope of *McConnell IV* in *Collins v. Athens Orthopedic Clinic, P.A.*, 307 Ga. 555 (2019). In *Collins*, current and former patients sued a medical clinic

for negligence after their personal data was stolen from the clinic. While the Georgia Supreme Court's decision focused on the issue of injury, it "included an extended parenthetical explaining the specific holding of *McConnell* [*IV*]—namely that there was no duty under *Bradley Center*, nor under O.C.G.A. § 10-1-393.8 or O.C.G.A. § 10-1-910." *Purvis v. Aveanna Healthcare, LLC*, 2021 WL 5230753, at *3 (N.D. Ga. Sep. 27, 2021).

Notably, this Court did not rely on *Bradley Center* as the only, or even the primary, source of the duty to protect sensitive consumer information. Instead, its decision was animated by (1) strict federal regulation of the credit reporting industry and (2) the reasonable foreseeability of the risk to Equifax's data security systems. *See In re Equifax*, 362 F. Supp. 3d at 1323-25. As explained below, *McConnell IV* did not disturb these central pillars of the Court's duty of care analysis.

First, unlike the Georgia Department of Labor, "Equifax and the other national credit reporting agencies are heavily regulated by federal law." *Id.* at 1323. For example, the Gramm-Leach-Bliley Act ("GLBA") directed the Federal Trade Commission ("FTC") to promulgate standards for financial institutions

> (1) to insure the security and confidentiality of customer records and information;
> (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
> (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

15 U.S.C. § 6801(b). The ensuing Safeguards Rule requires credit reporting agencies

like Equifax to "develop, implement, and maintain a comprehensive information security program" that "contains administrative, technical, and physical safeguards[.]" 16 C.F.R. § 314.3; *see also Individual Reference Servs. Grp., Inc. v. FTC*, 145 F. Supp. 2d 6, 32 (D.D.C. Apr. 30, 2011) (holding a credit reporting bureau is a "financial institution under Subtitle A of the [GLBA] and is therefore subject to the FTC's rules under that subtitle"). In particular, regulated companies must designate a qualified individual to oversee and implement their security programs, conduct an assessment of internal and external risks to customer information, design and implement safeguards to control identified risks, regularly test the effectiveness of those safeguards, and establish a written incident response plan to promptly respond to and recover from any security event.[6] 16 C.F.R. § 314.4.

In addition to the GLBA, Section 5 of Federal Trade Commission Act ("FTCA") has been used to regulate corporate cybersecurity for the protection of consumer data.

---

[6] In *Wells Fargo Banks, N.A. v. Jenkins*, 293 Ga. 162, 165 (2013), the Georgia Supreme Court held that Section 501(a) of the GLBA does not impose a legal duty on a bank to protect its customers' confidential personal information. *See* 15 U.S.C. § 6801(a) ("It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."). The court interpreted Section 501(a) as a mere "aspirational statement of Congressional policy": "[i]t does not provide for certain duties or the performance of or refraining from any specific acts on the part of financial institutions, nor does it articulate or imply a standard of conduct or care, ordinary or otherwise." *Wells Fargo*, 293 Ga. at 164-65. However, the court did not take into account the Safeguards Rule in rejecting a legal duty under the GLBA. *Id.* at 165 n.3. By contrast, this Court's duty of care conclusion rests in part on the Safeguards Rule, which imposes specific data security obligations on financial institutions.

In relevant part, Section 5 prohibits "[u]nfair methods of competition" and "unfair or deceptive acts or practices in or affecting commerce[.]" 15 U.S.C. § 45(a). An act or practice may be deemed unfair if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." *Id.* § 45(n). In *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 240, 247 (3d Cir. 2015), the Third Circuit affirmed that the FTC may enforce Section 5 against companies whose deficient cybersecurity measures allow hackers to steal customers' personal and financial information. And in this district, one court has found that Section 5 creates an enforceable duty to safeguard personal data based on the statutory text and precedent in the data breach context. *Purvis*, 2021 WL 5230753, at *8. Given the GLBA's and the FTCA's concern with data theft and not merely intentional disclosure, the Court concludes that these statutes impose a duty of care on Equifax to keep the sensitive information stored on its networks secure.

Second, nothing in *McConnell IV* forbids a court to factor the foreseeability of the harm into the duty of care equation. In *McConnell I*, the Georgia Court of Appeals held that the Georgia Department of Labor owed no duty to protect personal data while distinguishing a federal data breach case in which this Court

> found a duty to protect the personal information of the defendant's customers in the context of allegations that the defendant failed to implement reasonable security measures to combat a substantial data security risk of which it had received multiple warnings dating back several years and even took affirmative steps to stop its employees from fixing known security deficiencies.

337 Ga. App. at 459 n.4. The *McConnell I* court noted that no such allegations were made in that case, *see id.*, and neither the Georgia Court of Appeals nor the Georgia Supreme Court has dispelled that distinction in three successive opinions.[7] *See In re Equifax*, 362 F. Supp. 3d at 1325; *McConnell*, 305 Ga. at 815-16 (omitting any mention of foreseeability in the duty of care discussion). Indeed, post-*McConnell IV* cases have found that the concept of foreseeability continues to play a role in defining legal duty under Georgia law. *See, e.g.*, *Purvis*, 2021 WL 5230753, at *4-5 (recognizing a duty "based on Defendant's alleged knowledge of the foreseeable risk of a data breach and the resulting exposure of Plaintiffs' information").

Here, Joshpe, Khalaf, Lee, and Patterson allege that Equifax knew or should have known about risks in its cybersecurity protocols but failed to take adequate measures to safeguard consumer information. (Equifax's Br. in Supp. of Equifax's

[7] Equifax submits the *McConnell* complaint to show that the plaintiff there did in fact allege that it was "reasonably foreseeable" that unauthorized third parties would access his personal information. (Reply Br. in Supp. of Equifax's Mot. to Dismiss, at 12 (quoting *id.*, Ex. 1 ¶¶ 26-27).) However, those allegations were conclusory and accompanied by no factual support, unlike the allegations of foreseeability made by Joshpe, Khalaf, Lee, and Patterson. (*See id.*, Ex. 1 ¶ 26 ("It was reasonably foreseeable that Defendant's failure to safeguard and protect Plaintiff's and the other Class Members' personal information would result in unauthorized third parties gaining access to Plaintiff's and the other Class Members' personal information.") *See also McCullough v. Finley*, 907 F.3d 1324, 1333 (11th Cir. 2018) (on a motion to dismiss, "[c]onclusory allegations are not entitled to the assumption of truth"). This Court will not presume that the Georgia Court of Appeals or the Georgia Supreme Court "credited" the *McConnell* allegations in the face of clear, contrary language in *McConnell I*. (*Contra* Reply Br. in Supp. of Equifax's Mot. to Dismiss, at 12.)

Mot. to Dismiss, Ex. 1, Pt. 3 at 5-7, 19-21, 37, 54.) In particular, according to Joshpe and Khalaf, hackers were able to scan Equifax's systems for a specific vulnerability in the Apache Struts Web Framework which the United States Computer Emergency Readiness Team had publicly identified in March 2017. (*Id.*, Ex. 1, Pt. 3 at 5-6, 19-21.) Lee further alleges that Equifax failed to upgrade its cybersecurity by installing a remedial patch from a software maker, and that Equifax knew hackers routinely attempted to steal the valuable data on its systems. (*Id.*, Ex. 1, Pt. 3 at 37.) Similarly, Patterson states that, prior to the Data Breach, there were four instances when hackers accessed Equifax data between 2013 and 2017 due to the company's technical errors. (*Id.*, Ex. 1, Pt. 3 at 54.) As the Court held with respect to the Consumer Plaintiffs, the alleged foreseeability of the Data Breach supports a duty of care on Equifax's parts to safeguard the personal data in its custody. *See In re Equifax*, 362 F. Supp. 3d at 1325.

2. Injury

The Court turns next to Equifax's arguments that Joshpe, Khalaf, Lee, and Patterson have not alleged any cognizable injuries to sustain their negligence claims. First, Equifax contends that the economic loss rule prohibits recovery for actual or attempted fraud, increased risk of identity theft, identity theft mitigation efforts, and reputational damage. (Equifax's Br. in Supp. of Equifax's Mot. to Dismiss, at 19-20.) "The economic loss rule generally provides that a contracting party who suffers purely economic losses must seek his remedy in contract and not in tort. In other words, a

plaintiff may not recover in tort for purely economic damages arising from a breach of contract." *In re Equifax*, 362 F. Supp. 3d at 1321 (quotation marks and citations omitted). However, the rule does not bar a tort claim where the defendant has breached an established duty of care independent of any contract. *See id.* (citing *Liberty Mut. Fire Ins. Co. v. Cagle's, Inc.*, 2010 WL 5288673, at *3 (N.D. Ga. Dec. 16, 2010)); *Johnson v. 3M*, 2021 WL 4745421, at *30 (N.D. Ga. Sep. 20, 2021). Because Equifax owed a duty to protect consumers' personal data from cybertheft, the negligence claims of Joshpe, Khalaf, Lee, and Patterson are not subject to the economic loss rule.

Equifax also argues that Joshpe and Khalaf cannot recover (1) emotional distress damages without having suffered some physical impact from the Data Breach or (2) reputational damages absent intentional or wanton misconduct by Equifax. (*Id.* at 20 n.11, 21.) "In a claim concerning negligent conduct, a recovery for emotional distress is allowed only where there is some impact on the plaintiff, and that impact must be a physical injury." *Ryckeley v. Callaway*, 261 Ga. 828, 828 (1992). "On the other hand, where the conduct is malicious, wilful or wanton, recovery can be had without the necessity of an impact"—but only if the complained-of conduct was "directed toward" the plaintiff. *Id.* at 828-29. Similarly, reputational damages "are recoverable only in actions alleging intentional or wanton misconduct, for example, libel and slander, malicious prosecution or malicious arrest." *Hamilton v. Powell, Goldstein, Frazer & Murphy*, 167 Ga. App. 411, 416 (1983), *aff'd*, 252 Ga. 149

(1984). As with emotional distress damages, the tort examples given in *Hamilton* suggest that intentional or wanton misconduct must be targeted at the plaintiff to warrant reputational damages. Here, Joshpe and Khalaf have not alleged that the Data Breach caused them any physical injuries, nor have they alleged that Equifax directed any malicious, willful, or wanton misconduct at them. They thus cannot seek damages for emotional distress or reputational harm on their negligence claims.

Finally, Equifax argues that "[t]he risk of future identity theft alleged by . . . Patterson and Lee [is] too speculative to establish a cognizable injury, because their Complaints contain no factual allegations to 'plausibly infer that' they 'likely will suffer identify theft.'" (Equifax's Br. in Supp. of Equifax's Mot. to Dismiss, at 21 (alterations and emphasis omitted) (quoting *Collins*, 307 Ga. at 562).) Under Georgia law, "[a] wrongdoer is not responsible for a consequence which is merely possible, according to occasional experience, but only for a consequence which is probable, according to ordinary and usual experience." *Collins*, 307 Ga. at 558 (citation and alteration omitted). In *Collins*, the Georgia Supreme Court held that victims of a data breach had pleaded a plausible risk of identity theft based on allegations that

> (1) a thief stole a large amount of personal data by hacking into a business's computer databases and demanded a ransom for the data's return, (2) the thief offered at least some of the data for sale, and (3) all class members now face the "imminent and substantial risk" of identity theft given criminals' ability to use the stolen data to assume the class members' identities and fraudulently obtain credit cards, issue fraudulent checks, file tax refund returns, liquidate bank accounts, and open new accounts in their names.

Id. at 562. According to the court, "showing injury as a result of the exposure of data

is easier in a case like this, where the data exposure occurs as a result of an act by a criminal whose likely motivation is to sell the data to others." *Id.*

Patterson's and Lee's allegations that the criminal theft of their personal data exposes them to a substantial risk of identity theft, puts this case on all fours with *Collins*. In her complaint, Patterson asserts that (1) "her sensitive [PII] was STOLEN" in "the fraudulent Data Breach that was allowed by EQUIFAX," and (2) "the preventable EQUIFAX Security Data Breach intensifies [a] substantial risk of identity theft and aggravated identity theft harm, injury, and damage for [her][.]" (Equifax's Br. in Supp. of Equifax's Mot. to Dismiss, Ex. 1, Pt. 3 at 49, 55.) Lee provides even greater detail in support of her alleged future harms, including that (1) "Equifax allowed unauthorized criminal computer hackers to obtain consumer reports of [hers]"; (2) "[t]here are reports that information from the Equifax Data Breach is already on sale on . . . the Dark Web"; (3) "stolen data may be held for up to a year or more before being used to commit identity theft"; and (4) she "faces [a] significant risk of harm or threat of harm in the future" from identity theft and associated fraud. (*Id.*, Ex. 1, Pt. 3 at 37-39.) The Court concludes that these allegations, accepted as true, are sufficient to survive a motion to dismiss on the issue of injury.

3. Proximate Causation

Equifax also seeks to dismiss Joshpe's and Khalaf's negligence claims for lack of proximate causation. (*Id.* at 23-25.) Both Joshpe and Khalaf allege that they

"possessed outstanding credit ratings" until the Data Breach, after which they experienced multiple instances of identity theft and fraud. (*Id.*, Ex. 1, Pt. 3, at 7-8, 21-22.) According to Equifax, these allegations "do not *establish* that it is more likely than not that the [Data Breach]—as opposed to any other breach or exposure of their information—caused their alleged harms." (*Id.* at 24 (emphasis added) (quotation marks, citation, and emphasis omitted).) But this argument impermissibly elevates the standard of review on a motion to dismiss: "allegations can establish nothing, and . . . a plaintiff does not need to 'establish' any facts nor present any evidence to meet its modest burden of stating a plausible claim for relief." *Charleston Waterkeeper v. Frontier Logistics, L.P.*, 488 F. Supp. 3d 240, 252 (D.S.C. 2020). Nor must Joshpe and Khalaf "explicitly state that other breaches did *not* cause these injuries, since their allegations that this Data Breach *did* cause their injuries implies such an allegation." *In re Equifax*, 362 F. Supp. 3d at 1318 (emphasis in original). The Court then will not dismiss Joshpe's and Khalaf's negligence claims on causation grounds.

F. FCRA

Equifax contends that Joshpe, Khalaf, Lee, and Patterson cannot maintain their FCRA claims because Equifax did not "furnish" any consumer reports in the Data Breach.[8] (*Id.* at 28-29.) This argument is consistent with the Court's earlier

[8] Although the Defendants include Patterson in the list of Opt-Out Plaintiffs asserting FCRA claims, the Court finds no such claim pleaded anywhere in her complaint. (Defs.' Br. in Supp. of Defs.' Mot. to Dismiss, Ex. 1, Pt. 3 at 49-57.) Nevertheless, to the extent her complaint does raise a claim for relief under the

holding that information "stolen from a credit reporting agency is not 'furnished' within the meaning of the FCRA." *In re Equifax*, 362 F. Supp. 3d at 1312. Here, the allegations show only that criminal hackers stole the Opt-Out Plaintiffs' sensitive personal data, not that Equifax actively transmitted any consumer reports to a third party. *Id.* at 1312-13 (noting the term "furnish" is used "to describe the active transmission of information to a third-party rather than a failure to safeguard the data") (citation omitted). Moreover, the information allegedly stolen during the Data Breach was not a "consumer report" as defined in the FCRA. *Id.* at 1313. Joshpe, Khalaf, and Lee allege that their names, social security numbers, birth dates, addresses, driver's license numbers, and credit card information were exposed in the Data Breach. (Equifax's Br. in Supp. of Equifax's Mot. to Dismiss, Ex. 1, Pt. 3 at 1, 15, 36.) Courts have concluded that such information constitutes "header information," not a consumer report, because it does not bear on an individual's credit worthiness. *In re Equifax*, 362 F. Supp. 3d at 1313. For these reasons, the Court dismisses the Opt-Out Plaintiffs' claims under FCRA Sections 1681b and 1681e.

G. Suggestion for Remand

Following the partial grant of Equifax's Motion to Dismiss, the only claims remaining in this MDL are those asserted by Joshpe, Khalaf, Lee, and Patterson for negligence and violations of state consumer protection statutes. The Court suggests

---

FCRA, it would fail for the same reasons discussed herein.

that the Judicial Panel on Multidistrict Litigation ("Panel") remand these claims to their transferor courts for final resolution. Under 28 U.S.C. § 1407(a), each transferred action "shall be remanded by the [P]anel at or before the conclusion of such [coordinated or consolidated] pretrial proceedings to the district from which it was transferred[.]" Although the Panel alone is vested with authority to remand a case, it "has consistently given great weight to the transferee judge's determination that remand of a particular action at a particular time is appropriate because the transferee judge, after all, supervises the day-to-day pretrial proceedings." *In re Brand-Name Prescription Drugs Antitrust Litig.*, 170 F. Supp. 2d 1350, 1352 (J.P.M.L. 2001) ("*Prescription Drugs*") (citation omitted). Indeed, there is an expectation that the transferee court will suggest remand to the Panel once it perceives its role to be completed under section 1407. *See In re Light Cigarettes Mktg. Sales Pracs. Litig.*, 832 F. Supp. 2d 74, 76 (D. Me. 2011) ("*Light Cigarettes*").

Generally speaking, the decision of whether to remand a case or claim turns on "the totality of circumstances involved in that docket." *Prescription Drugs*, 170 F. Supp. 2d at 1352. Section 1407 does not contemplate that a "transferee judge will necessarily complete all pretrial proceedings in all actions transferred and assigned to him by the Panel[.]" *In re Evergreen Valley Project Litig.*, 435 F. Supp. 923, 924 (J.P.M.L. 1977). To the contrary, the Panel "has the discretion to remand a case when everything that remains to be done is case-specific," or when it "will serve the convenience of the parties and witnesses and will promote the just and efficient

conduct of the litigation." *In re Patenaude*, 210 F.3d 135, 145 (3d Cir. 2000) (citation and alteration omitted); *see also In re Activated Carbon-Based Hunting Clothing Mktg. & Sales Pracs. Litig.*, 840 F. Supp. 2d 1193, 1198 (D. Minn. 2012) ("*Hunting Clothing*") ("[W]hether to remand turns on whether the case will benefit from further coordinated proceedings as part of the MDL.") (quotation marks, citation, and alteration omitted); *United States ex rel. Hockett v. Columbia/HCA Healthcare*, 498 F. Supp. 2d 25, 38 (D.D.C. 2007) ("[T]he decision of whether to suggest remand should be guided in large part by whether one option is more likely to insure the maximum efficiency for all parties and the judiciary.") (quotation marks and citation omitted).

Applied here, the Court believes that those principles weigh in favor of remanding the few cases left in this MDL to their original courts. As explained above, the Consumer Plaintiffs and Equifax have reached a class action settlement of all claims arising out of the Data Breach, which was approved more than two years ago and upheld in substantial part on appeal. Of the 14 Consumer Plaintiffs who opted out of the settlement, this Order narrows that number to just four single-plaintiff cases with two claims each. There are no efficiencies or other benefits to be had from consolidating "only small, simple actions" in this Court. *Hunting Clothing*, 840 F. Supp. 2d at 1199 (quotation marks, citation, and alteration omitted); *see also In re State St. Bank & Tr. Co. Fixed Income Funds Inv. Litig.*, 2011 WL 1046162, at *5 (S.D.N.Y Mar. 22, 2011) ("[C]ase-specific rulings are neither the purpose, nor the forte of a court presiding over a[n MDL]."); *Light Cigarettes*, 832 F. Supp. 2d at 78 ("This

leaves only four remaining cases, substantially lessening the prospect of inconsistent determinations of common issues and the inconvenience and expense of multiple-jurisdiction litigation."); *In re Ford Motor Co. Bronco II Prod. Liab. Litig.*, 1998 WL 308013, at *2 (E.D. La. June 8, 1998) (suggesting remand where "the claims of all but a handful of named plaintiffs have been dismissed"). Instead, "matters that relate to only a few cases . . . should be decided by the court that will actually conduct the trial." *In re Bisphenol-A (BPA) Polycarbonate Plastic Prods. Liab. Litig.*, 276 F.R.D. 336, 339 (W.D. Mo. 2011).

Also, although there is some factual and legal overlap in the remaining cases, all four involve claims under either New York or California law that are inherently less familiar to this Court than the transferor courts. Those claims—and Equifax's arguments to dismiss them—raise plaintiff- and state-specific questions about, for example, whether delayed notice of the Data Breach can be "materially misleading" under NYGBL Section 349, and what is required to allege "incremental harm" under the CCRA. (Equifax's Br. in Supp. of Equifax's Mot. to Dismiss, at 32-37.) This Court has not gained any particular expertise on these matters from its supervision of the litigation; instead, "the transferor courts, each of which is familiar with the state law of their respective jurisdictions, are in a better position to assess the parties' state law arguments[.]" *Light Cigarettes,* 2011 WL 6151510, at *4; *accord Tennessee Med. Ass'n v. United Healthgroup Inc.*, 2014 WL 12837582, at *5 (S.D. Fla. Jan. 16, 2014); *Hunting Clothing*, 840 F. Supp. 2d at 1199. Accordingly, the Court denies the Motion

to Dismiss as to Joshpe's, Khalaf's, and Lee's NYGBL Section 349 claims and Patterson's CCRA claim without prejudice.

IV. Conclusion

For the foregoing reasons, the Defendants' Motion to Dismiss [Doc. 1220] is GRANTED with respect to Douglas Adams [No. 1:19-cv-3682-TWT], Alice Flowers [No. 1:10-cv-5703-TWT], Edward Hutchinson [No. 1:19-cv-5706-TWT], Ruby Hutchinson [No. 1:19-cv-5705-TWT], Raymond Silva [No. 1:19-cv-3825-TWT], Christopher Eustice and Cathy Eustice [No. 1:19-cv-3128-TWT], Christopher Eustice and David Eustice [No. 1:19-cv-3129-TWT], and Christopher Eustice and Travis Hubbard [No. 1:19-cv-3130-TWT]. The Court GRANTS in part and DENIES in part the Defendants' Motion to Dismiss [Doc. 1220] with respect to Audella Patterson [No. 1:19-cv-5529], Brett Joshpe [No. 1:19-cv-3595-TWT], Richard Khalaf [No. 1:19-cv-3830], and Anna Lee [No. 1:18-cv-4698-TWT].

The Court suggests to the Judicial Panel on Multidistrict Litigation that the actions of Audella Patterson [No. 1:19-cv-5529](Central District of California), Brett Joshpe [No. 1:19-cv-3595-TWT](Southern District of New York), Richard Khalaf [No. 1:19-cv-3830](Southern District of New York), and Anna Lee [No. 1:18-cv-4698-TWT](Eastern District of New York) be remanded to the transferor courts as indicated for further proceedings. This Order essentially terminates this MDL proceeding.

SO ORDERED, this 13th day of April, 2022.

THOMAS W. THRASH, JR.
United States District Judge